CONTINUATION IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Trisha M.A. Kovac, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, depose and state as follows:

INTRODUCTION

1. I have been employed as a Special Agent ("SA") of the Federal Bureau of Investigation since February 1, 2009, and am currently assigned to the Detroit Division, Saint Joseph Resident Agency. While employed by the FBI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography, and regularly assist in the prosecution of these types of cases. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including coercion and enticement and traveler offenses. As a federal agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. My duties include the investigation of alleged violations of federal criminal laws, including matters involving violations of 18 U.S.C. §§ 2251 and 2252A (which make it illegal to produce, distribute, and possess child pornography in interstate commerce) and of 18 U.S.C. § 2423 (which makes it illegal to travel in interstate commerce with the intent to engage in illicit sexual activity).

2. Pursuant to the provisions of 18 U.S.C. § 2256(8), "child pornography" means a visual depiction, the production of which involves the use of a minor engaging in sexually explicit

conduct, including but not limited to various simulated or actual sex acts, or the lascivious exhibition of the genitals or the pubic area.

3. Based on the information set forth below, there is probable cause to believe that evidence of violations of federal law, specifically, 18 U.S.C. §§ 2251 and 2252A (which make it illegal to produce, distribute, and possess child pornography in interstate commerce) and of 18 U.S.C. § 2423 (which makes it illegal to travel in interstate commerce with the intent to engage in illicit sexual activity) will be found on certain electronic devices, specifically: (1) **a Google Pixel 2 phone with IMEI 357536087171205 and S/N: FA7BH1A00357, Model G011A; and (2) a Black ASUS Notebook Laptop, Model Q524U** (hereinafter the **"Subject Devices,"** described more fully in Attachment A). The categories of electronically stored information and evidence sought are described in Attachment B.

4. The statements contained in this continuation are based in part on information provided by U.S. federal law enforcement agents, written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement officers, information gathered from investigative sources of information, and my experience, training, and background as a Special Agent.

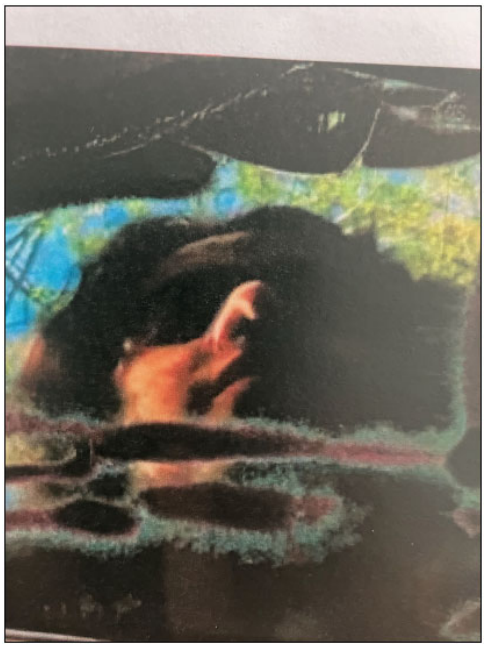
5. This continuation is submitted for the limited purpose of securing a search warrant. I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of federal law are located on the **Subject Devices.**

FACTUAL BACKGROUND OF INVESTIGATION

6. On or around April 14, 2023, 11:30 a.m., a woman herein referred to as W.J. contacted the Berrien Springs Oronoko Township Police Department to report that her 12-year-old daughter, herein referred to as J.R., had left the house after W.J. went to work at 5:00 a.m. According to information obtained by J.R.'s sister from J.R.'s Snapchat account, J.R. went to meet a male in his twenties known only as "Jessy" to have sex in the woods for drugs. At the time she went missing, J.R. was wearing a purple hoodie with neon-colored graphics of a skeleton hand holding a rose, and grey shorts.

7. Afterward, J.R.'s sister found a video in J.R.'s Snapchat account, which is an account with username noregrets-cea1, that showed her having sex with a Hispanic male in the woods. The video had been sent to J.R.'s Snapchat account from account jessy225827[1] that morning and was shot from the perspective of the male subject. The video at first appeared to be in the "portrait" mode, and a male's face can be seen clearly. The camera view then flips, and a close-up of intercourse of a penis penetrating a vagina is visible. A female can be seen having her hair pulled while she is in the all-fours position from the male vantage point taking the video. J.R.'s sister identified the female as J.R. based upon her physical appearance and the shirt she was wearing in the video. A screen capture from the video showed the below subject:

[1] A preservation request was submitted to Snapchat for noregrets-cea1 and jessy225827 on April 18, 2023 and April 15, 2023, respectively.



8. FBI was notified shortly after 4:00 pm that same day that J.R. was missing, and initiated a number of emergency disclosure requests to track her location and identify the subject. An emergency disclosure request submitted to Snapchat for jessy225827 returned Google email account mtorres.12349@gmail.com and IP logs returning to Verizon Wireless.[2] A search in Accurint[3] for mtorres.12349@gmail.com returned a match for an individual identified as EDUARDO G. TORRES, DOB xx/xx/1997, residential address in Waukegan, IL.[4] An emergency disclosure request submitted to Google, LLC for mtorres.12349@gmail.com requesting all

[2] Snapchat is a visual social media messaging application operated by Snap Inc., a company located in Santa Monica, California.

[3] Accurint is a public record database that law enforcement routinely uses in investigations.

[4] The full date of birth and street address are known to me, but I have not included them to protect personal identifying information.

account information, including subscriber and location information, provided location data that indicated that the account had traveled from outside Chicago, Illinois to Berrien Springs, Michigan from 1 a.m. to 4 a.m., spent time in the vicinity of J.R.'s address, then traveled towards Benton Harbor, MI, leaving at approximately 4:00 p.m. eastern time to return to Chicago. The timing of the Google location data shows that the subject was in the vicinity of either Berrien Springs or Eau Claire, Michigan at the time Snapchat user jessy225827 sent the video of sexual intercourse to J.R.'s Snapchat account.

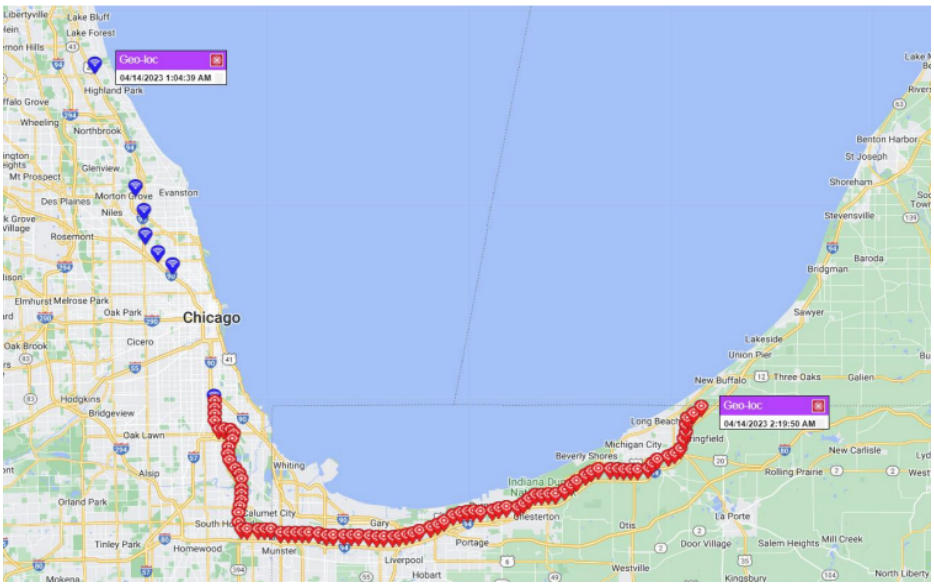
9. Google returned the following subscriber information for mtorres.12349@gmail.com:

Eddie Torres
Waukegan, IL
224-406-4664

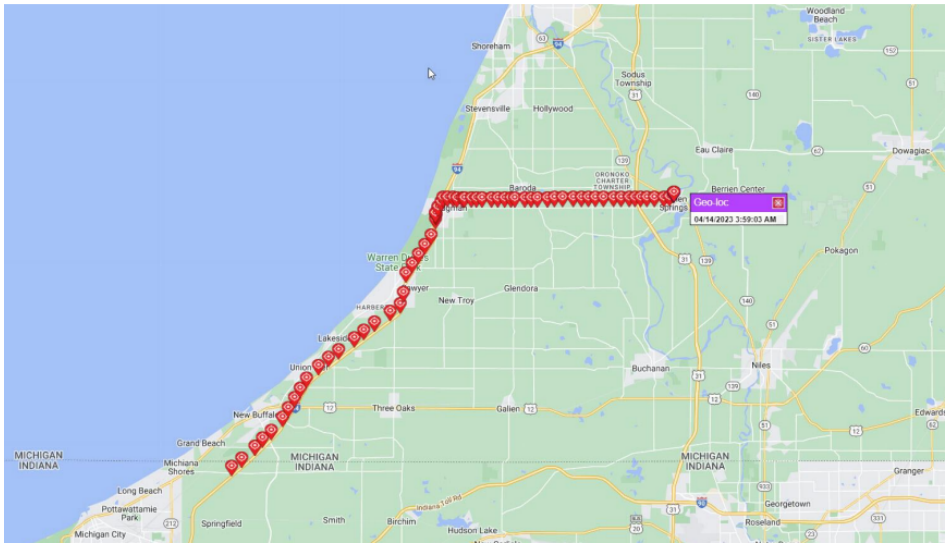
The street address in Waukegan provided by Google matched the street address in Accurint, and the same phone number was also linked to TORRES in Accurint.

10. The location history of the Google account was plotted onto maps by an FBI Special Agent from the Cellular Analysis Survey Team (CAST), which provided TORRES's travel history, as shown below:

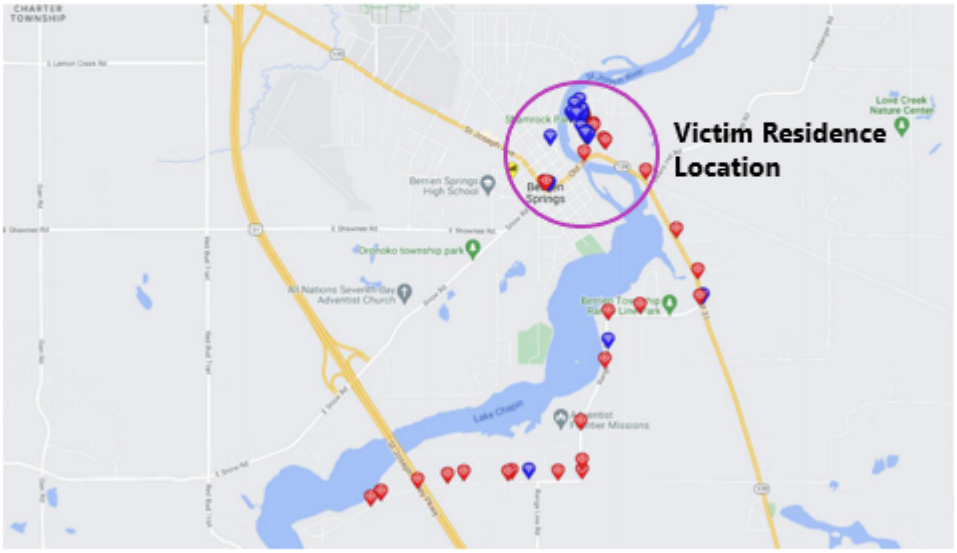
Mtorres.12349@gmail.com
Google Location History
4/14/2023 1:00 AM to 3:00 AM



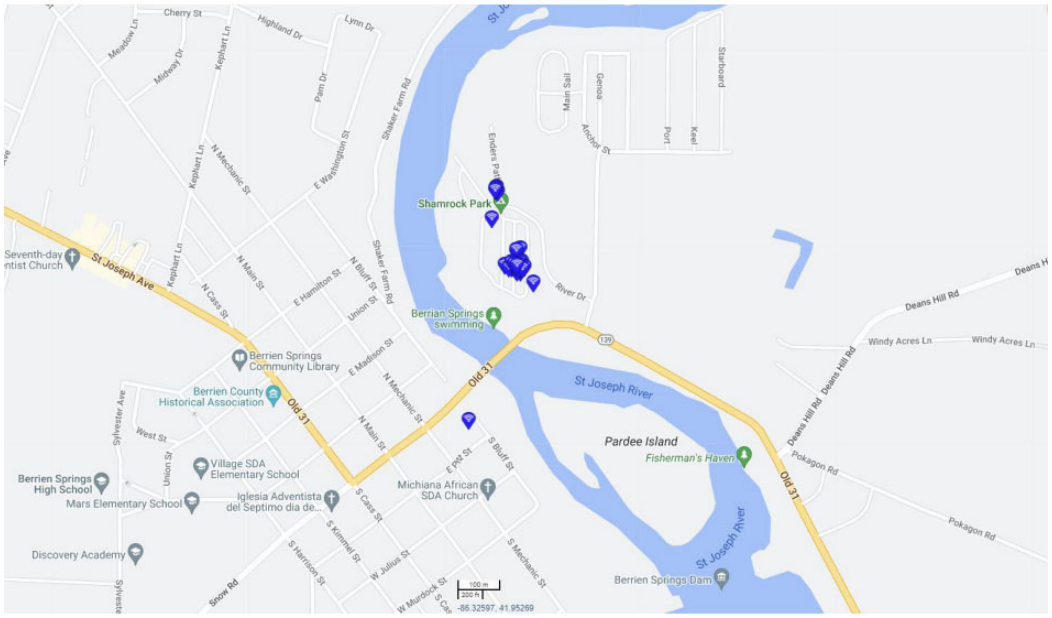
Mtorres.12349@gmail.com
Google Location History
4/14/2023 3:00 AM to 4:00 AM



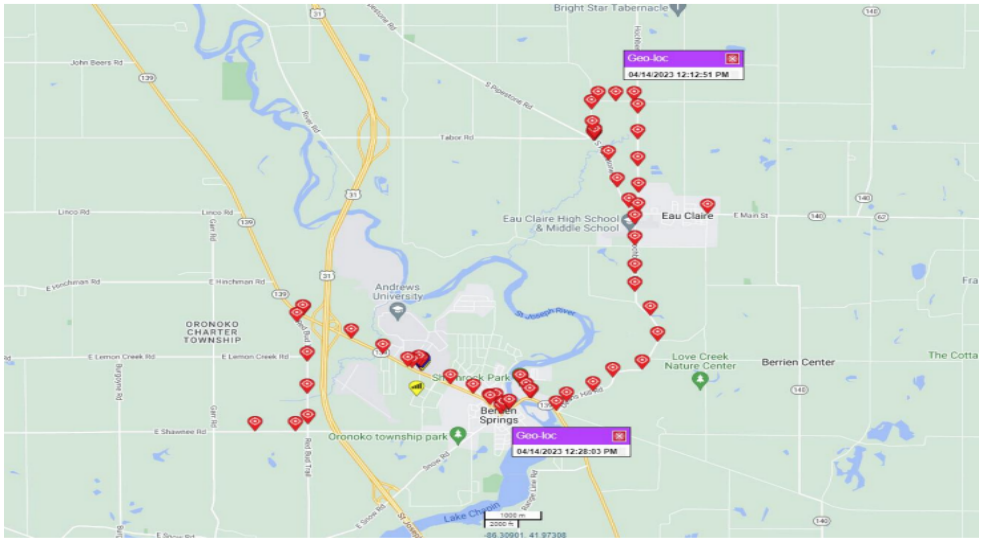
Mtorres.12349@gmail.com
Google Location History
4/14/2023 4:00 AM to 8:00 AM



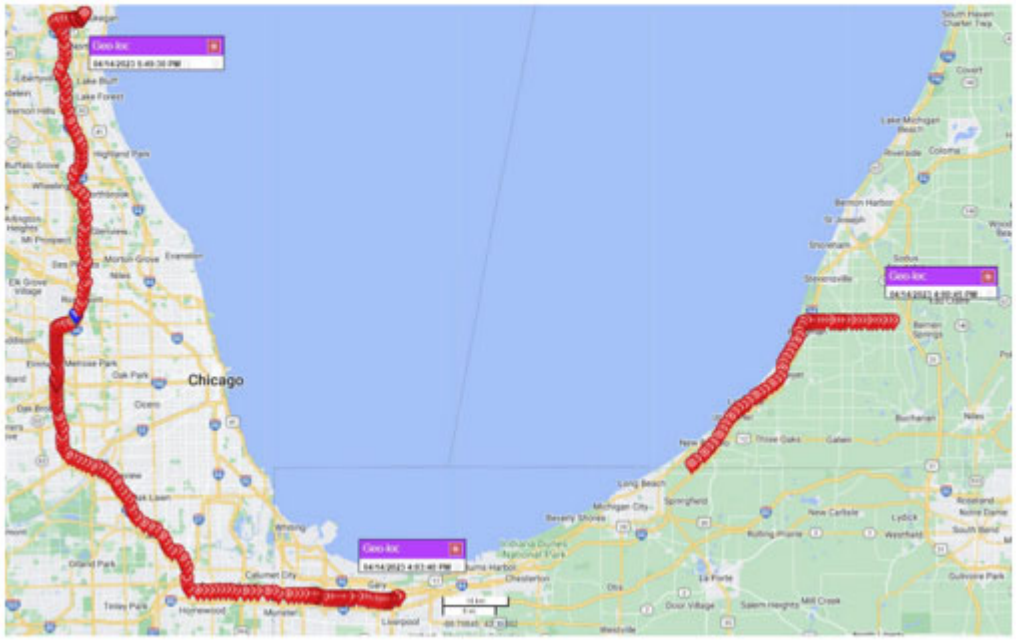
Mtorres.12349@gmail.com
Google Location History
4/14/2023 8:00 AM to 12:00 PM



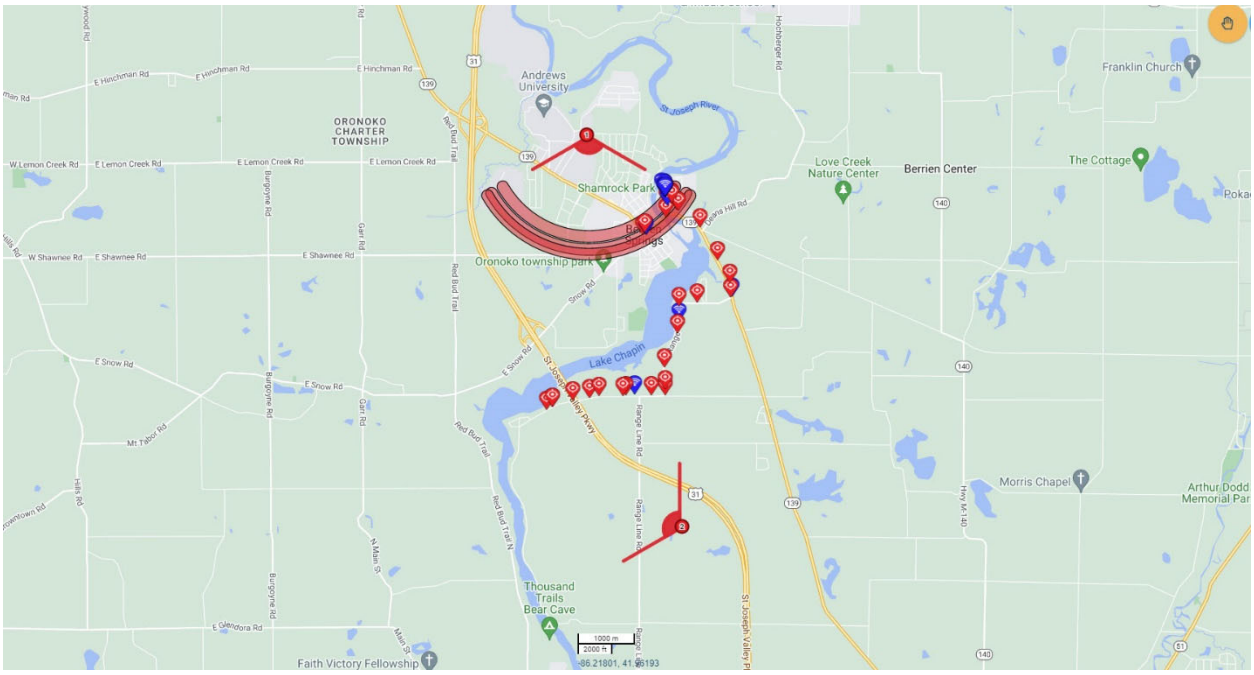
Mtorres.12349@gmail.com
Google Location History
4/14/2023 12:00 PM to 4:00 PM



Mtorres.12349@gmail.com
Google Location History
4/14/2023 4:00 PM to 6:49 PM



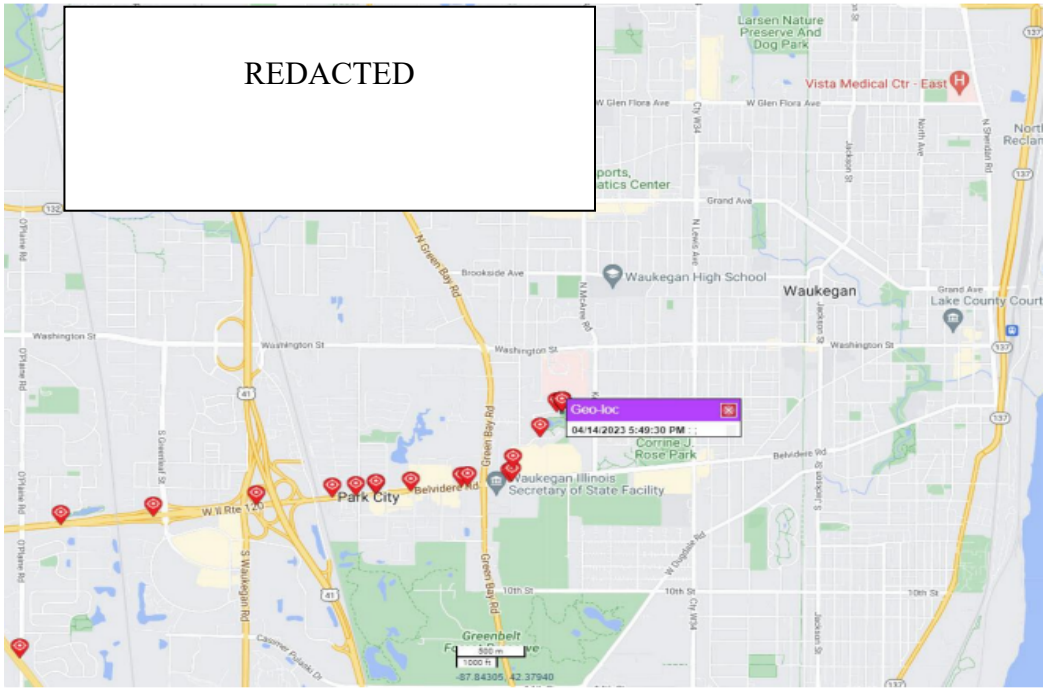
11. The FBI submitted an exigent request to Verizon for subscriber information for the cellular account number 224-406-4464. This number was associated with EDUARDO G. TORRES both in Accurint and from the Google account information listing the subscriber as Maria Torres at the same address in Waukegan, IL. According to the Chicago Department of Motor Vehicles, Maria Torres's DOB is xx/xx/1969.[5] Law enforcement contacted Maria Torres at the Waukegan address and confirmed that she is TORRES's mother. Location information provided by Verizon for cellular account number 224-406-4464 also showed the same path of travel as the Google account data showed. A combined image of the Verizon and Google data shows both the Google account and the Verizon account located within the vicinity of J.R.'s residence between 4:00 a.m. and 6:00 a.m. on April 14, 2023:



[5] The full date of birth is known to me, but I have not included it to protect personal identifying information.

12. As of 6:49 p.m. on April 14, 2023, the Google account gave the following location within the city of Waukegan, IL:

Mtorres.12349@gmail.com
Google Location History
6:49 PM (EST)



13. An Illinois driver's license for EDUARDO G. TORRES shows an individual of similar appearance to the male from the video:

14. From the late hours of April 14, 2023, to the early morning hours of April 15, 2023, cellular number 224-406-4464 continued to ping within the vicinity of the known Waukegan, IL address for EDUARDO G. TORRES. In the early morning hours of April 15, 2023, Agents approached the residence and observed individuals outside of the residence who identified themselves as family members of TORRES. TORRES and J.R. were seated in a vehicle in the driveway.

15. Upon making contact with TORRES, Agents called 224-406-4464, and heard the phone ring in TORRES's pocket, which he picked up. Agents seized the device, which was a **Google Pixel 2 phone with IMEI 357536087171205 and S/N: FA7BH1A00357, Model G011A.** Google Pixel phones are not manufactured in Michigan. Agents read TORRES his *Miranda* rights and interviewed him. TORRES admitted that he was communicating with J.R. on Snapchat with the purpose of driving to Michigan to see her to engage in sexual intercourse. He stated that he

had not met her in person prior to April 14, 2023. TORRES admitted that he traveled to Michigan to pick up J.R. and that he had sexual intercourse with J.R. twice, including once in the woods near J.R.'s residence in Berrien Springs, Michigan. TORRES stated that he waited until J.R.'s mother left for work to pick up J.R. After TORRES and J.R. had sexual intercourse, he admitted that he drove her across state lines to his home in Waukegan, Illinois.

16. Additionally, TORRES admitted to producing three videos of himself and J.R. having sexual intercourse and that he sent those videos to J.R.'s Snapchat account. A portion of one of the videos has been recovered by law enforcement after J.R.'s sister located the video (described above) on J.R.'s Snapchat account. TORRES admitted that he believed that J.R. was 13 years old. TORRES admitted that he had a laptop at his residence on which he had viewed child sexual abusive materials in the past. Agents also seized the computer, which is a **Black ASUS Notebook Laptop, Model Q524U**. TORRES further admitted to talking to others who he believed were minors on Snapchat and stated that J.R. was the first he had met in person. Based on the location data evidence, the Snapchat video evidence, and TORRES's statements, including that the first time he met J.R. in person was on April 14, 2023, the video of sexual intercourse was produced in Berrien County in the Southern Division of the Western District of Michigan when he had sex with J.R. in the woods near her residence. TORRES was subsequently arrested.

17. On April 15, 2023, the government filed a criminal complaint against TORRES for violations of 18 U.S.C. §§ 2251(a) (production of child pornography); 2252A(a)(5)(B) (possession of child pornography); 2423(a) (transportation of a minor); and 2423(b) (travel with intent to engage in illicit sexual activity). (1:23-mj-00162-RSK PageID.2).

BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET

18. Based on my training, experience, and information obtained from other agents, I know the below statements are accurate.

19. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

20. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as WiFi or Bluetooth. Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

21. Any computer can connect to any smartphone, tablet, or other computer. Through the internet, electronic contact can be made to millions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

22. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - computer hard drives, external hard drives, CDs, DVDs, and thumb, jump, or flash drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital

camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

23. The internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

24. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

25. Individuals commonly use smartphone and computer apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored.

26. Communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (e.g., temporary files or ISP client software,

among others). In addition to electronic communications, a computer user's internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS COMMON TO INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

27. Based on my knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals interested in a sexual relationship with children. Characteristics common to people interested in having a sexual relationship with children include that they:

a. Generally have a sexual interest in children and receive sexual gratification from viewing children engaged in sexual activity or in sexually suggestive poses, or from literature describing such activity.

b. May collect sexually explicit or suggestive materials in a variety of media, including in hard copy and/or digital formats. People with a sexual interest in children oftentimes use these materials for their own sexual arousal and gratification. They may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse or groom a child to participate in sex, or to demonstrate the desired sexual acts.

c. May also keep "trophies" or mementos of sexual encounters with children, or items that they use to gratify a sexual interest in children, such as by collecting children's underwear or other items belonging to a child.

d. May take photographs that either constitute child pornography or indicate a sexual interest in children by using cameras, video cameras, web cameras, and cellular telephones. Such

images and video may be taken with or without the child's knowledge. This type of material may be used by the person to gratify a sexual interest in children.

e. Generally, maintain their communication indicating a sexual interest in children and child pornography in a safe, secure, and private environment, most often where they live and/or on their person. These images and videos can be downloaded onto desktop or laptop computers, computer disks, disk drives, data disks, system disk operating systems, magnetic media floppy disks, internet-capable devices, cellular telephones, tablets, digital music players, and a variety of electronic data storage devices (hardware, software, diskettes, tapes, CDs, DVDs, SD cards, memory cards, USB/jump/flash memory devices, external hard drives, and other digital storage media). The images can be stored in both digital and hard copy format and are usually hidden so that they are not found by other members of the individual's family.

f. May correspond with and/or meet others to share information and materials; rarely destroy correspondence from others with a sexual interest in children; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, screen names, and telephone numbers of individuals with whom they have been in contact and who share the same sexual interest in children. Such correspondence may take place, for example, through online bulletin boards and forums, internet-based chat messaging, email, text message, video streaming, letters, telephone, and in person.

SPECIFICS OF SEIZING AND SEARCHING COMPUTER AND PHONE EVIDENCE

28. The warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

29. I know based on my knowledge, training, and experience that:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium or electronic device that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in what is commonly referred to as a swap or recovery file;

b. Computer or phone files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. When a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data;

c. Wholly apart from user-generated files, computer or phone storage media—in particular, internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer or phone users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information; and

d. Files that have been viewed via the internet are sometimes automatically downloaded into a temporary internet directory or cache.

30. As further described in Attachment B, this application seeks permission to locate not only device files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how devices were used, the purpose of their use, who used them, and when. Probable cause exists that this forensic electronic evidence will be on the **Subject Devices.**

31. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer or phone file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

32. Information stored within a computer, phone, and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience,

information stored within a computer, phone, or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer, phone, or storage media.

33. This user attribution evidence is analogous to the search for indicia of occupancy while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer or phone owner. Further, computer, phone, and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers and phones typically contain information that logs user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the device, and the IP addresses through which the device accessed networks and the internet. Such information allows investigators to understand the chronological context of device access, use, and events relating to the crime under investigation.

34. Some information stored within a computer, phone, or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer or phone may both show a particular location and have geolocation information incorporated into its file data. Such file data also typically contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The

geographic and timeline information described herein may either inculpate or exculpate the computer user.

35. Information stored within a computer or phone may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information within the device may indicate the owner's motive and intent to commit a crime (*e.g.*, internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

36. A person with appropriate familiarity with how a computer or phone works can, after examining this forensic evidence in its proper context, draw conclusions about how devices were used, the purpose of their use, who used them, and when.

37. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer and phone evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer or phone is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

38. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a

storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

39. I know that when an individual uses a computer or phone to obtain or access child pornography, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer or phone used to commit a crime of this type may contain data that is evidence of how the device was used, data that was sent or received, notes as to how the criminal conduct was achieved, records of internet discussions about the crime, and other records that indicate the nature of the offense.

40. Computer and phone users can attempt to conceal data within equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension .jpg often are image files. A user can easily change the extension to .txt to conceal the image and make it appear that the file contains text. Computer and phone users can also attempt to conceal data by using encryption. Encryption involves the use of a password or device, such as a dongle or keycard, to decrypt the data into readable form.

41. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit imaging, or otherwise copying the **Subject Devices** and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium.

This might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

42. I respectfully submit that there is probable cause to believe that EDUARDO G. TORRES has violated 18 U.S.C. §§ 2251 and 2252A (which make it illegal to produce, distribute, and possess child pornography in interstate commerce) and of 18 U.S.C. § 2423 (which makes it illegal to travel in interstate commerce with the intent to engage in illicit sexual activity). I submit that this application supplies probable cause for a search warrant authorizing the examination of the **Subject Devices** described in Attachment A to seek the items described in Attachment B.

43. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).